

Amendment Under 37 C.F.R. §1.116
Serial No. 10/069,118
Attorney Docket No. 020234

REMARKS

Claims 23-63 are pending in the above-identified application. Applicants amend claims 23, 24, 26, 28, 31, 34, 35, 37, 43-51, 53-59. No new subject matter is added. It is respectfully submitted that this Amendment is fully responsive to the Office Action dated November 29, 2005.

Claims 23-63 were rejected under 35 U.S.C. §112. In rejecting these claims, the Examiner remarked:

- 1) The claims do not disclose how the first decryption key is generated and obtained;
- 2) The encrypted content key was already decrypted at a first decryption processing unit and why is there a need for a second decryption processing unit to extract the content key?
- 3) The structure of the system is confusing and the Examiner is not able to distinguish what cryptographic keys are used for its respective functions.

Applicants respectfully disagree with each of the Examiner's remarks 1-3 and emphasize that the claims are clearly written and in proper form.

1) To expedite prosecution, Applicants hereby amend claim 23 to more clearly recite how the first decryption key is generated and obtained (e.g., the first decryption key refers to private decryption key K_p corresponding to the public encryption key K_{Pp} and that the private decryption key K_p is a preset key, unique to the cellular phone that corresponds to the data reproduction apparatus, and is not generated, e.g., page 10, line 20 to page 11, line 11 as well as on page 11, line 32 to page 13, line 4.)

2) Applicants respectfully submit that there is a need for a second decryption processing unit to extract the content key in the present invention. For instance, the encryption content key refers to encryption content key [Kc] Kp, and corresponds to content key Kc encrypted with private description key Kp. Therefore, in order to decrypt encryption content data [Dc] Kc, content key Kc must be extracted. Moreover, second decryption processing unit 1530 decrypts encryption content key [Kc] Kp using private decryption key Kp to extract content key Kc, and third decryption processing unit 1520 decrypts encryption content data [Dc] Kc using content key Kc to extract content data Dc. This description is supported, for example, on page 10, line 20 to page 11, line 11 in the specification (e.g., Fig. 7 and p. 14, lines 20-29.)

3) Applicants respectfully submit that the structure of the system is *not* confusing, and that it is clear from the claim language, how cryptographic keys are used for its respective functions. However, to expedite prosecution and assist the Examiner, Applicants hereby explain, with the following examples, the encryption key approach corresponding to each independent claim.

(i) For example, the invention according to independent claim 23 is related to a configuration similar to Fig. 4 in the present application.

Cellular phone 200 corresponds, for example, to a data reproduction apparatus that includes an audio reproduction module 1500 corresponding to, for example, a data reproduction unit, and a memory card 120 corresponding to, for example, a data storage unit.

Memory card 120 corresponds, for example, to a data storage unit that stores encryption content data [Dc] Kc and encryption content key [Ke] Kp.

Audio reproduction module 1500 is directed to, for example, a configuration including a session key generation unit 1502 generating a session key Ks, an encryption processing unit 1504 encrypting session key Ks using public encryption key K_{Pm} unique to memory card 120 and provide that key to memory card 120, a decryption processing unit 1506 decrypting encryption content key [[Kc] Kp] Ks encrypted with session key Ks using session key Ks to extract encryption content key [Kc] Kp, a Kp hold unit 1540 prestoring private decryption key Kp corresponding to the first decryption key, a decryption processing unit 1530 decrypting encryption content key [Kc] Kp using private decryption key Kp to extract content key Kc, and a decryption processing unit 1520 decrypting encryption content data [Dc] Kc using content key Kc to extract content data Dc.

In brief, for example, data reproduction unit 1500 provides to memory card 120 an encrypted session key Ks that is updated at every access. At memory card 120, encryption content key [[Kc] Kp] is further encrypted using session key Ks to be transmitted to data reproduction unit 1500.

Data reproduction unit 1500, for example, possesses session key Ks and private decryption key Kp, and carries out decryption to extract content key Kc. Encryption content data [Dc] Kc, for example, is decrypted using content key Kc to extract content data Dc.

Since the decryption key and data in plain text cannot be looked from an external source in accordance with the configuration of the present invention, it will be difficult to obtain the

encryption system and private decryption key of cellular phone 200 illegally from an external source. Thus, the present invention provides, for example, the advantage of improving security.

(ii) For example, the invention according to claim 28 is related to a configuration similar to Figs. 8 and 12 of the above-identified application.

Cellular phone 300 (400), for example, corresponds to a data reproduction apparatus that includes an audio reproduction module 1500 corresponding to a data reproduction unit, and a memory card 130 (140) corresponding to a data storage unit.

Memory card 130 (140), for example, corresponds to a data storage unit stores encryption content data $[D_c] K_c$ and content key K_c . First session key K_{s2} , for example, is encrypted so as to be decryptable by private decryption key K_p corresponding to a unique decryption key for output to audio reproduction module 1500.

Audio reproduction module 1500 includes, for example, a K_p hold unit 1540 prestoring private decryption key K_p corresponding to a unique decryption key, a decryption processing unit 1530 carrying out a decryption process using private decryption key K_p , a session key generation unit 1552 generating second session key K_{s1} , an encryption processing unit 1554 encrypting second session key K_{s1} using first session key K_{s2} that has been decrypted at decryption processing unit 1530 for output to memory card 130 (140), and a decryption processing unit 1556 using second session key K_{s1} to decrypt content key $[[K_c] K_p] K_{s1}$ that has been encrypted so as to be decryptable by private decryption key K_p and that has been encrypted with second session key, such that encryption content key $[K_c] K_p$ is extracted.

Decryption processing unit 1530, for example, decrypts encryption content key $[K_c] K_p$

by private decryption key K_p to extract content key K_c .

Audio reproduction module 1500, for example, decrypts encrypted content data $[D_c] K_c$ using content key K_c that has been extracted at decryption processing unit 1530 to extract content data D_c .

For instance, in brief, memory card 130 encrypts session key K_{s2} that is generated at that memory card at every access for output to data reproduction unit 1500. Data reproduction unit 1500 extracts session key K_{s2} , which is used to encrypt session key K_{s1} that is updated at every access, and provides the encrypted key to memory card 120. At memory card 130, encryption content data $[K_c] K_{p1}$ is further encrypted using session key K_{s1} to be transmitted to data reproduction unit 1500.

Data reproduction unit 1500, for example, possesses session key K_{s1} and private decryption key K_p , which are used for decryption to extract content key K_c . Encryption content data $[D_c] K_c$ is decrypted by content key K_c to extract content data D_c .

Since the decryption key and data in plain text cannot be looked from an external source in accordance with the configuration of the present invention, it will be difficult to obtain the encryption system and private decryption key of cellular phone 300 (400) illegally from an external source. The present invention provides, for example, the advantage of improving security.

The security is further improved, for example, by using two session keys K_{s1} and K_{s2} that are updated at every access.

(iii) For example, the invention according to claim 34 is related to a configuration similar

to Figs. 16 and 19 of the above-identified application.

Cellular phone 500 (600), for example, corresponds to a data reproduction apparatus that includes an audio reproduction module 1500 corresponding to a data reproduction unit, and a memory card 150 (160) corresponding to a data storage unit.

Memory card 150 (160), for example, corresponds to a data storage unit stores encryption content data [Dc] Kc and content key Kc. First session key Ks2 is encrypted so as to be decryptable using private decryption key Kp corresponding to a unique decryption key for output to audio reproduction module 1500.

Audio reproduction module 1500, for example, is directed to a configuration including a Kp hold unit 1540 prestoring private decryption key Kp corresponding to the unique decryption key, a decryption processing unit 1530 extracting first session key Ks2 using private decryption key Kp, a session key generation unit 1552 generating second session key Ks1, an encryption processing unit 1554 encrypting second session key Ks1 using first session Ks2 that has been decrypted at decryption processing unit 1530 for output to memory card 150 (160), a decryption processing unit 1556 decrypting content key [Kc] Ks1 encrypted with second session key Ks1 using second session key Ks1 to extract content key Kc, and a decryption processing unit 1520 decrypting encrypted content data [Dc] Kc using content key Kc extracted at decryption processing unit 1556 to extract content data Dc.

For example, in brief, memory card 130 encrypts session key Ks2 that is generated at that memory card at every access, and provides the encrypted key to data reproduction unit 1500.

Data reproduction unit 1500 extracts session key Ks2, which is used to encrypt session key Ks1

that is updated at every access for output to memory card 120. At memory card 130, content key Kc is encrypted using session key Ksl to be transmitted to data reproduction unit 1500.

Data reproduction unit 1500, for example, possesses session key Ksl which is used for decryption to extract content key Kc. Encrypted content data [Dc] Kc, for example, is decrypted using content key Kc to extract content data Dc.

Since the decryption key and data in plain text cannot be looked at from an external source in accordance with the configuration of the present invention, it will be difficult to obtain the encryption system and private decryption key of cellular phone 500 (00) illegally from an external source. The present invention, for example, provides the advantage of improving security.

The security is further improved, for example, by using two session keys Ksl and Ks2 that are updated at every access.

(iv) For example, the invention related to claim 45 is related to a configuration of audio reproduction module 1500 similar to Figs. 16 and 19 of the above-identified application.

Audio reproduction module 1500, for example, is directed to a configuration including a Kp hold unit 1540 prestoring private decryption key Kp corresponding to the unique decryption key, a decryption processing unit 1530 extracting first session key Ks2 using private decryption key Kp to decrypt first session key [Ks2] Kp that has been encrypted so as to be decryptable by private decryption key Kp that is supplied from a source external to audio reproduction module 1500, a session key generation unit 1552 generating second session key Ksl, an encryption processing unit 1554 encrypting second session key Ksl using first session Ks2 that has been

decrypted at decryption processing unit 1530 for output to a source external to audio reproduction module 1500, a decryption processing unit 1556 using second session key Ks1 to decrypt content key [Kc] Ks1 encrypted with second session key Ks1 that is supplied from a source external to audio reproduction module 1500 to extract content key Kc, and a decryption processing unit 1520 decrypting encrypted content data [Dc] Kc using content key Kc extracted at decryption processing unit 1556 to extract content data Dc.

In brief, data reproduction unit 1500, for example, decrypts externally applied encrypted session key Ks2 to extract session key Ks2, which is used to encrypt session key Ks1 that is updated at every access for output to an external source.

Externally applied encrypted content key [Kc] Ks1 is decrypted, for example, using session key Ks1 to extract content key Kc. Encryption content data [Dc] Kc is decrypted, for example, using content key Kc to extract content data Dc.

For example, since the decryption key and data in plain text cannot be looked at from an external source in accordance with the configuration of the present invention, it will be difficult to obtain the encryption system and private decryption key of audio reproduction module 1500 illegally from an external source. The present invention provides the advantage of improving security.

The security is further improved, for example, by virtue of using two session keys Ks1 and Ks2 that are updated at every access.

(v) For example, the invention related to independent claim 53 is related to a configuration similar to Figs. 8, 12, 16 and 19 of the above-identified application.

For example, a cellular phone 300 (400, 500, 600) corresponding to a data reproduction apparatus reproducing encrypted content data [Dc] Kc is directed to a configuration loaded with memory card 130 (140, 150, 160) storing encryption content data [Dc] Kc and content key Kc to encrypt first session key Ks2 so as to be decryptable using private decryption key Kp corresponding to a unique decryption key for output to cellular phone 300 (400, 500, 600).

Cellular phone 300 (400, 500, 600), for example, is directed to a configuration loaded with memory card 130 (140, 150, 160), and includes an interface 1200 for data transfer, a Kp hold unit 1540 to prestore private decryption key Kp corresponding to a unique decryption key, a decryption processing unit 1530 extracting first session key Ks2 using private decryption key Kp, a session key generation unit 1552 generating second session key Ksl, an encryption processing unit 1554 providing second session key Ksl to memory card 150 (160) using first session key Ks2, a decryption processing unit 1556 using second session key Ksl to decrypt content key [Kc] Ksl that is encrypted with second session key Ksl to extract content key Kc, and a decryption processing unit 1520 decrypting encryption content data [Dc] Kc using content key Kc extracted at decryption processing unit 1556 to extract content data Dc.

For example, in brief, cellular phone 300 (400, 500, 600) loaded with memory card 130 (140, 150, 160) decrypts session key Ks2 that has been generated at that memory card for every access to extract session key Ks2, and encrypts session key Ksl updated at every access using session key Ks2 for output to memory card 130 (140, 150, 160).

Cellular phone 300 (400, 500, 600), for example, decrypts content key [Kc] Ksl that has been encrypted using session key Ksl to extract session key Ksl. Then, encryption content data

Amendment Under 37 C.F.R. §1.116
Serial No. 10/069,118
Attorney Docket No. 020234

[Dc] Kc is decrypted by content key Kc to extract content data Dc.

Since the decryption key and data in plain text cannot be looked at from an external source in accordance with the configuration of the present invention, it will be difficult to obtain the encryption system and private decryption key of cellular phone 300 (400, 500, 600) illegally from an external source. The present invention provides the advantage of improving security.

The security is further improved, for example, by using two session keys Ks1 and Ks2 that are updated at every access.

Applicants respectfully submit that the claims are presented in a clearly understandable form and distinctly claim the invention. Thus, in view of the above remarks and the remarks in the previous Amendment, Applicants' respectfully request that the Examiner withdraw the §112 rejections. Applicants submit that that the claims, as herein amended, are in condition for allowance. Applicants request such action at an early date.

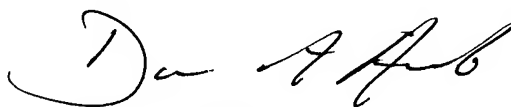
If the Examiner believes that this application is not now in condition for allowance, the Examiner is requested to contact Applicants' undersigned attorney to arrange for an interview to expedite the disposition of this case.

Amendment Under 37 C.F.R. §1.116
Serial No. 10/069,118
Attorney Docket No. 020234

If this paper is not timely filed, Applicants respectfully petition for an appropriate extension of time. The fees for such an extension or any other fees that may be due with respect to this paper may be charged to Deposit Account No. 50-2866.

Respectfully submitted,

WESTERMAN, HATTORI, DANIELS & ADRIAN, LLP

A handwritten signature in black ink, appearing to read "Darrin A. Auito". The signature is fluid and cursive, with the first name "Darrin" being more prominent than the last name "Auito".

Darrin A. Auito
Attorney for Applicants
Registration No. 56,024
Telephone: (202) 822-1100
Facsimile: (202) 822-1111

DAA/meu